



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/524,358	03/14/2000	Tateo Oishi	450100-02402	8951
20999	7590	01/14/2009	EXAMINER	
FROMMER LAWRENCE & HAUG 745 FIFTH AVENUE- 10TH FL. NEW YORK, NY 10151			NALVEN, ANDREW L	
ART UNIT		PAPER NUMBER		
2434				
MAIL DATE		DELIVERY MODE		
01/14/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	09/524,358	OISHI ET AL.
Examiner	Art Unit	
ANDREW L. NALVEN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 31 October 2008.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-6,8-17 and 19-21 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-6, 8-17, 19-21 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 14 March 2000 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

1. Claims 1-6, 8-17, 19-21 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-6, 8-17, and 19-21 have been considered but are not persuasive.

3. Applicant has argued on page 5 that the combination of Yoshiura and Keith fails to teach an encryption block having a second data length that is smaller than the unit of the compression block having the first data length. Examiner respectfully disagrees.

Applicant states that Yoshiura discloses "compressing data into a block size and encryption of the compressed data block" (see Remarks Page 5). Given this interpretation, it is clear that Yoshiura teaches a larger block being compressed into a smaller block because compression reduces the size of data. The smaller block is then encrypted. Thus, Yoshiura teaches an encryption block having a second data length that is smaller than the unit of the compression block having the first data length.

Yoshiura lacks a teaching that the compression block length is an integer multiple greater than the encryption block length. Keith cures this defect by teaching a first data length being an integral multiple greater than one of the second data length thus providing a smaller unit of length for a subsequent encryption block than the compression block's first data length (Keith, column 1 lines 20-25, Huffman encoding

creates a compression ratio of 2). As a result, Examiner maintains that the combination of Yoshiura and Keith teach an encryption block having a second data length that is smaller than the unit of the compression block having the first data length.

4. Applicant further argues on pge 7 that Yuenyongsgool fails to teach the storing of blocks in the order of encryption by consecutive addresses. Examiner respectfully disagrees. Yuenyongsgool teaches the storing of blocks in the order of encryption by consecutive addresses (Yuenyongsgool, column 2, lines 38-45, column 4 lines 42-67). Yeunyongsgool teaches that encrypted data is typically kept in consecutive addresses because of the principle of locality.

5. Applicant further argues on page 8 that the combination of Yoshiura, Keith, and Bahout fails to teach the first data length is able to replay audio/visual data. Examiner respectfully disagrees. Keith discloses the use of huffman encoding for compression (Keith, Abstract). Keith further discloses that this encoding procedure is used in video processing for replaying video (Keith, column 1 lines 10-25 and lines 36-55).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3-4, 6, 13,15-16, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720 in view of Keith US Patent No. 5,615,020 and Park US Patent No. 5,761,302.

8. With regards to claims 1, 13 and 21, Yoshiura teaches processing means for compressing data in units of a compression block having a first data length (Yoshiura, column 4 lines 38-48), encrypting means for encrypting the compressed data in units of an encryption block having a second data length (Yoshiura, column 4 lines 48-58), wherein the first data length is a data length of an integer multiple of the second data length (Yoshiura, column 4 lines 48-49, integer multiple is 1), and control means for writing the encrypted data in said storage means so that the data positioned in the same encryption block is also positioned in the same compression block, said control means reading the data from said storage means in units of the compression block (Yoshiura, column 4 lines 56-58, column 8 lines 15-17). Yoshiura fails to teach the data being audio/visual data, the first data length being an integral multiple greater than one of the second data length, and separating each block into a plurality of units and encrypting each unit. However, Examiner maintains that it would have been obvious to one of ordinary skill in the art to apply Yoshiura's compression and encryption methods to audio/visual data because it would offer the advantage of reducing the storage space requirements of large audio/visual data files and would provide security for valuable intellectual property through encryption. Further, Keith teaches a first data length being an integral multiple greater than one of the second data length thus providing a smaller unit of length for a subsequent encryption block than the compression block's first data

length (Keith, column 1 lines 20-25, Huffman encoding creates a compression ratio of 2). Further, Park teaches separating each compression block into a plurality of units and encrypting each unit (Park, column 5 lines 44-58, compressed MPEG data is divided into encryption blocks and encrypted). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Keith's method of compressing to a ratio of 2 and Park's method of encryption because it offers the advantage of minimizing the average code length for Huffman encoding and compressing data into smaller data sets (Keith, column 1 lines 10-25) and providing flexibility in encryption because smaller encryption blocks allow for varying of keys and encryption techniques to increase the difficulty of cryptanalysis (Park, column 6 lines 49-54).

9. With regards to claims 3, 15, Yoshiura as modified teaches an encryption process using the block to be encrypted and a ciphertext from the previous block in the form of cipher-block chaining (Yoshiura, column 5 lines 5-12).

10. With regards to claims 4 and 16, Yoshiura as modified teaches control means that manages the encrypted data stored in said storage means using a cluster containing one or more compression blocks and values initially used when encrypted an encryption block in one of said compression blocks (Yoshiura, column 4 lines 48-58, work key).

11. With regards to claim 6, Yoshiura as modified teaches the control means outputting data read out in compression block units into the processing means (Yoshiura, column 8 lines 15-17).

12. Claims 2 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720, Park US Patent No. 5,761,302 and Keith US Patent No. 5,615,020, as applied to claims 1 and 13 above, and in further view of Bellovin et al US Patent No. 5,241,599.

13. With regards to claims 2 and 14, Yoshiura as modified above fails to teach the inserting of data into the processing block in order to adjust the data length so that it becomes a whole number multiple of the predetermined length. Bellovin teaches the insertion of data in order to meet the predetermined length of a block (Bellovin, column 10, lines 24-30). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bellovin's method of inserting data because it offers the advantage of helps prevent partition attacks against encryption keys (Bellovin, column 9 line 54 – column 10 line 47).

14. Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720, Park US Patent No. 5,761,302 and Keith US Patent No. 5,615,020, as applied to claim 4 above, and further in view of Yuenyongsgool US Patent No. 6,202,152.

15. With regards to claims 5 and 17, Yoshiura as modified fails to teach the storing of blocks in the order of encryption at consecutive addresses. However, Yuenyongsgool teaches the storing of blocks in the order of encryption by consecutive addresses (Yuenyongsgool, column 2, lines 38-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Yuenyongsgool's

method of consecutive address storage because it offers the advantage of helping accelerate information transfers from encrypted memory (Yuenyongsgool, column 2, lines 4-23).

16. Claims 8, 10-11, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720 in view of Keith US Patent No. 5,615,020, Park US Patent No. 5,761,302 and Bahout et al US Patent No. 5,594,793.

17. With regards to claim 8, 19, 20, Yoshiura as modified above in the rejection of claim 1 fails to teach a system for mutual identification between the storage and data processing apparatuses. However, Bahout teaches a system for mutual identification between the storage and data processing apparatuses using stored keys and algorithms within the data processor (Bahout, column 7, lines 7-25). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bahout's mutual identification method because it offers the advantage of giving the system a degree of inviolability by ensuring that data processor only functions with a specific storage device (Bahout, column 1, lines 9-16 and 55-60).

18. With regards to claim 10, Yoshiura as modified teaches an encryption process using the block to be encrypted and a ciphertext from the previous block in the form of cipher-block chaining (Yoshiura, column 5 lines 5-12).

19. With regards to claim 11, Yoshiura as modified teaches control means that manages the encrypted data stored in said storage means using a cluster containing

one or more compression blocks and values initially used when encrypted an encryption block in one of said compression blocks (Yoshiura, column 4 lines 48-58, work key).

20. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720, Park US Patent No. 5,761,302, Keith US Patent No. 5,615,020, and Bahout et al US Patent No. 5,594,793, as applied to claim 8 above, and in further view of Bellovin et al US Patent No. 5,241,599.

21. With regards to claim 9, Yoshiura as modified above fails to teach the inserting of data into the processing block in order to adjust the data length so that it becomes a whole number multiple of the predetermined length. Bellovin teaches the insertion of data in order to meet the predetermined length of a block (Bellovin, column 10, lines 24-30). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bellovin's method of inserting data because it offers the advantage of helps prevent partition attacks against encryption keys (Bellovin, column 9 line 54 – column 10 line 47).

22. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura et al US Patent No 6,157,720, Park US Patent No. 5,761,302, Keith US Patent No. 5,615,020, and Bahout et al US Patent No. 5,594,793, as applied to claim 11 above, and further in view of Yuenyongsgool US Patent No. 6,202,152.

23. With regards to claim 12, Yoshiura as modified fails to teach the storing of processing blocks in the order of encryption at consecutive addresses. However,

Yuenyongsgool teaches the storing of compression blocks in the order of encryption by consecutive addresses (Yuenyongsgool, column 2, lines 38-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Yuenyongsgool's method of consecutive address storage because it offers the advantage of helping accelerate information transfers from encrypted memory (Yuenyongsgool, column 2, lines 4-23).

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Andrew L Nalven/
Primary Examiner, Art Unit 2434